Ji Jiang

Ethernet VPN Prototyping on Next Generation NPU

Comparison of VPLS and Ethernet VPN Technologies

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

April 15, 2015

Helsinki Metropolia University of Applied Sciences

Author	Ji Jiang
Title	Ethernet VPN prototyping on next generation NPU
Number of Pages	31 pages
Date	April 15, 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation Fields	Software Development and Networking
Instructors	Dr. Tero Nurminen, Principal Lecturer M.Sc. Jussi Katajala, Master Engineer

Ericsson Router 6000 Series is a new high-capacity router series for mobile backhaul network, which is under development currently. The next generation NPU is adopted by the router family products. Recently, a new technology, EVPN has emerged and has been reported to overcome some VPLS limitations. However, a detailed comparison of the EVPN and VPLS technologies has not been systematically done. Also, whether the next generation NPU supports EVPN feature is unknown. The purposes of this work are to compare the VPLS and EVPN technologies in detail, to discover the possibility of implementing EVPN on the next generation NPU, and to provide reliable references for future work.

The comparison is performed from the perspective of address learning, load balancing and services. By using the unified test bed, EVPN prototyping and testing are performed on the NPU, based on a typical EVPN topology and scenario. Ericsson Finland provides most of the resources and facilities for this study.

The results indicate that EVPN is superior to the VPLS technology in several aspects. By applying a combination of control plane and data plane address learning, the multi-homed flow-based load balancing and the integration of L2 and L3 services, the EVPN solution significantly improves the network resiliency and efficiency, compared to VPLS. Therefore, EVPN is strongly recommended on Router 6000 Series. The results also show that it is possible to implement an EVPN feature on the next-generation NPU.

Overall, this study provides pilot research results and valuable references for future implementation work. In the next step, more complicated topologies and scenarios of EVPN could be introduced and tested. Also the current testing environment could be enlarged to adapt to new conditions.

Keywords	EVPN, VPLS, comparison, prototyping, next generation NPU

Contents

Abbreviations

AC	Attachment Circuit
AD	Auto-discovery
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BOS	Bottom of Stack
BUM	Broadcast, Unknown Unicast and Multicast
CE	Customer Edge
DCI	Data Center Interconnect
DF	Designated Forwarder
DHCP	Dynamic Host Configuration Protocol
ENM	Ericsson Network Manager
ES	Ethernet Segment
ESI	Ethernet Segment Identifier
ESP	Encapsulating Security Payload
EVI	EVPN Instance
EVPN	Ethernet VPN
EXP	Experimental Field
FEC	Forwarding Equivalence Class
GPL	GNU General Public License
HVPLS	Hierarchical VPLS
IETF	Internet Engineering Task Force
ILM	Incoming Label Map
IP	Internet Protocol
IPsec	IP Security
IPOS	IP Network Operating System
LAC	L2TP Access Concentrator
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LNS	L2TP Network Server

LSP	Label Switched Path
LSR	Label Switch Router
L2F	Layer-2 Forwarding Protocol
L2TP	Layer-2 Tunneling Protocol
L2VPN	Layer-2 VPN
MAC	Media Access Control
MHD	Multi-homed Device
MHN	Multi-homed Network
MPLS	Multiprotocol Label Switching
MP-BGP	Multiprotocol BGP
MP2P	Multipoint-to-point
NAT	Network Address Translator
ND	Neighbor Discovery
NLRI	Network Layer Reachability Information
NPU	Network Processing Unit
N-PE	Network-facing PE
PBB	Provider Backbone Bridging
PE	Provider Edge
PPTP	Point-to-point Tunneling Protocol
PW	Pseudo-wire
P2MP	Point-to-multipoint
QoS	Quality of Service
RD	Route Distinguisher
RFC	Requests for Comments
RIB	Routing Information Base
RSVP-TE	Resource Reservation Protocol with Traffic Engineering
SA	Security Association
SDK	Software Development Kit
SHD	Single-homed Device
SHN	Single-homed Network
SNP 4000	Smart Network Processor 4000
SSL	Secure Sockets Layer
SSR	Smart Service Router

TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
U-PE	User-facing PE
VC	Virtual Circuit
VLAN	Virtual LAN
VPLS	Virtual Private LAN Services
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VXLAN	Virtual Extensible LAN

1 Introduction

Ericsson is the global leader of communication technologies and services. It provides comprehensive infrastructure, software and services in the information and communications technology for various industries, such as telecommunication operators. The products of Ericsson range from traditional and Internet Protocol networking equipment to mobile broadband, cable TV, video systems, and an extensive services operation. Ericsson greatly changed the world and people's lives during the last century and continues to bring people into an advanced telecommunication era nowadays. [1.]

The Internet is making our society increasingly networked. It provides people with infinite amount of data and contents; as well as connects people anywhere and anytime. Furthermore, future Internet would connect more things together in addition to people. As predicted by Ericsson, the number of global smartphone subscriptions would reach 6.1 billion and the connected devices 50 billion by the end of 2020. This will result in a huge growth of volume and diversity, regarding traffic, devices and applications. Thus, networks must become smarter than before. They must recognize customer devices, application types and customer settings, in order to maximize customer experience and realize efficient use of available network resources. Meanwhile, networks must become simpler and more resilient, allowing cheaper maintenance and minimum disruption during failure time. Therefore, a highly scalable and consolidated platform with sophisticated availability and resilience capabilities, which could minimize the probability and the potential impact of failures, is very necessary in our modern networks. [1; 2.]

Under these circumstances, Ericsson introduced an industry-leading IP service delivery platform consisting of the Smart Service Router (SSR) family of products in March, 2013. Driven by the Smart Network Processor 4000 (SNP 4000), a revolutionary network processor, SSR becomes a genuine multi-application platform which could deliver layer-two to layer-seven services with predictable performances. Located close to the core network, SSR realizes complete network convergence between network access types, so that subscribers can access services from any locations or devices. The proven operating

system of SSR offers functional convergence for all network functions, which greatly simplifies operations and reduces the cost of ownership. [2.]

To complement its existing router portfolio, Ericsson introduced Router 6000 Series, a new high-capacity router series for mobile backhaul and metro access networks, in March 2015. As an important part in Ericsson's next-generation router portfolio, the series realizes the uniform IP network operating system (IPOS) running on a comprehensive suite of platforms across the whole network. Meanwhile, Router 6000 Series combines with Ericsson Network Manager (ENM) to offer the telecommunication operators with unified management and control of the transport and radio network, easier deployment and higher operational efficiency. Moreover, it is integrated with Ericsson's other products and meets the LTE Advanced and 5G requirements. [3.]

The Router 6000 Series utilize next-generation network processing unit (NPU) [3]. Basically, all the features on the router device have to be implemented upon the availability of the network processor. Getting familiar with the features of the network processor and the application programming interface (API) of the hardware SDK is fundamental for the router software development. Today, with the growing use of Virtual Private Network (VPN), many manufactures have started deploying VPN connectivity on routers. It is required by Ericsson's customers as well. Virtual Private LAN Services (VPLS), a layer-two MPLS VPN technology, provides attractive VPN possibilities. However, VPLS has its existing limitations. Recently, a new technology, the Ethernet VPN (EVPN) has emerged and has been reported to be a promising solution to overcome those limitations [27]. However, a comparison of EVPN and VPLS technologies has not been performed systematically. Also, whether the EVPN feature is supported by the next generation NPU is still unknown.

The goals of the project are to compare the VPLS and EVPN technologies in detail, to discover EVPN advantages compared to VPLS, to find out the potential EVPN availability on the next generation NPU, and to provide a reliable reference for future development of the EVPN feature on Ericsson Router 6000 Series.

In the thesis work, I mainly focus on the theoretical studies and the comparison of EVPN and VPLS technologies, and the practical EVPN prototyping on the next generation NPU.

2 Theoretical Background

2.1 Virtual Private Network

Since the Internet is a cheap and widespread backbone infrastructure, more and more entities plan to build a secure virtual private network across a public network nowadays. Exempted from the cost of the traditional leased line and dial-up modems connections, VPN substitutes the early private data communication methods. VPN is a private network utilizing the public network to carry the traffic. Due to the low cost and significantly improved bandwidth provided by new technology such as fibre-optic networks, VPNs based on IP and IP/MPLS networks have been considered genuine private networks. VPNs could be classified into types of remote-access and site-to-site connectivity that are realized by different technologies. [4.]

In order to prevent private data from being viewed or tampered while travelling over public networks, VPNs normally permit exclusively authenticated remote access and make use of encryption technologies. Other techniques such as tunnelling and compression are used to achieve the security of VPNs. Tunnelling is a technology encapsulating the header and data fields of one protocol packet inside the payload field of another protocol, so that the final packet could transfer through the network that the original packet could not. [6.] Figure 1 is the basic model of VPN tunnel under the Internet.

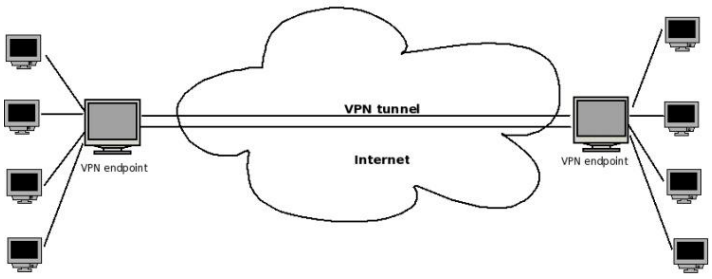

Figure 1. Basic model of VPN tunnel under Internet.
Copied from “Creating VPNs with IPsec and SSL/TLS” [6].

One example is that VPNs utilize the Internet Protocol Security (IPsec) framework to provide confidentiality, data integrity and endpoint authentication. IPsec was originally

generated by Internet Engineering Task Force (IETF) for IPv6. However it is commonly used by IPv4 and the Layer-two Tunnelling Protocol (L2TP) due to the slow deployment of IPv6. When a VPN is created, IPsec tunnel mode is used, which means every IP packet is completely encapsulated in a freshly created IPsec packet. Also, devices at the end of the tunnel de-encapsulate it and forward it to the desired destination. [5; 6.]

Tunnelling protocols are utilized to provide VPN functionality by allowing a foreign protocol to traverse through a network that does not support it. Layer-two tunnelling protocol (L2TP) is an example tunnelling protocol to support VPNs. L2TP is derived from point-to-point tunnelling protocol (PPTP) and layer-two forwarding protocol (L2F). [7.] A new version, L2TP version 3 (L2TPv3), is defined in IETF RFC 3931 in 2005. Since it cannot offer enough authentication and confidentiality, IPsec is normally adopted to secure the L2TP packets. L2TP tunnel carries PPP sessions. Also, the whole L2TP packet is transferred inside a UDP datagram. L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS) consist of two endpoints of a L2TP tunnel. LAC initializes the tunnel, and LNS waits for new tunnels. The data flow between the two endpoints is bidirectional after a tunnel is created. L2TP/IPsec VPN is set up by establishing a secure channel first and then a L2TP tunnel. In order to create a secure channel, IPsec security association (SA) has to be negotiated, before Encapsulating Security Payload (ESP) communication is established in transport mode. At last, L2TP tunnel could be created between the two SA endpoints. [8; 9.]

Another major implementation of VPNs is OpenVPN. It is an open-source software application project established by James Yonan and published under the GNU General Public License (GPL) [10]. Generally OpenVPN is used to create safe network-to-network and point-to-point connections in bridged or routed configurations and remote access. It offers a VPN solution based on secure sockets layer (SSL) / transport layer security (TLS). SSL and its successor TLS are cryptographic protocols providing safe data communications over public networks. It enables traversing network address translators (NATs) and firewalls, which is achieved by UDP encapsulation of ESP packet in IPsec implementation. [6; 10.]

2.2 Multiprotocol Label Switching

General IP unicast routing is based only on the destination address. It is not scalable to maintain routes on a source destination. Regarding traffic engineering, adjusting routing metrics could be done solely on the aggregated flow in the IP unicast. To optimize the efficiency and capability of traffic flow, the multiprotocol label switching (MPLS) is a more manageable and scalable solution to this. [11, 54.] The MPLS uses the mechanism of carrying data from one network device to another according to the short path labels instead of the long IP address. A variety of network protocols could be supported by MPLS. [12.]

The MPLS is considered a “layer 2.5” protocol since it locates between the traditionally defined network layer and the data link layer. An important feature of the MPLS is the clear separation of control and forwarding. All of the control modules in the MPLS are using the same quality of service (QoS) paradigm. Furthermore, the forwarding algorithm is completely independent of control modules, so that it could be made easy and efficient. The control modules in an MPLS, for example, include VPNs, multicast routing, unicast routing, frame delay, traffic engineering and so on. [11, 55.]

MPLS introduces sophisticated routing control capabilities into IP networks. It is realized by the adoption of label-switched path (LSP), and is determined at by FEC in the original device. Label edge router (LER) is the beginning of LSP, which is also called ingress router. It uses the routing information to decide which label to prefix to a packet. Label switch router (LSR) lies inside an MPLS network and uses a lookup table to determine the next hop in the LSP and the correct label. The old label is replaced by the new one before the packet is routed forward. The last LER in the LSP is named the egress router. It strips the label from the packet and forwards the packet according to the next layer header. [13, 44-45.]

An MPLS header including an arbitrary number of labels is allowed to be prefixed to the packet. The labels are simply stacked, named as a label stack. Figure 2 shows the length and location of MPLS label stack in an Ethernet/IP packet. As it indicates, a MPLS label value is 20 bits long by itself. When encapsulated, there are 3 “experimental field” bits, 1 “bottom-of-stack” bit, and 8 “time to live” (TTL) bits after the label value bits. The swap,

push and pop operations of a MPLS label mean that a new control element is acting on the packet. In addition, one advantage of MPLS is that it permits one to several control components take action on a packet. Since the label lookup and switching are happening in the switch instead of CPU, it is much swifter than a routing table or routing information base (RIB) lookup. [11, 55; 14, 78.]

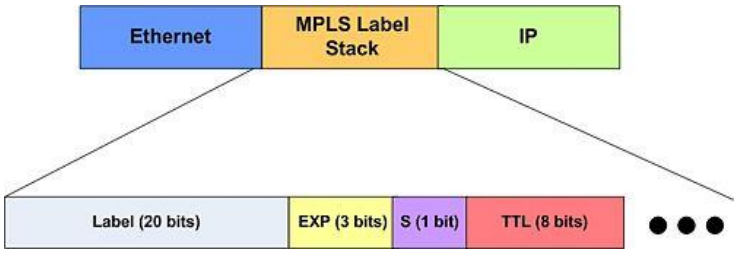

Figure 2. MPLS label stack in an Ethernet/IP packet. Copied from “OpenFlowMPLS” [16].

Nowadays service providers are driven to deploy more multicast services than before. A multicast service is one of the key challenges that MPLS faces. Many multiservice service providers have deployed MPLS in a controlled way, so that they could maximize the efficiency of delivery of multipoint streams. In the example of TV channels, IP/MPLS over a single point-to-multipoint (P2MP) LSP can deliver the service from the root to the relays. Another example is the application of high-quality IP multipoint video conferences. Moreover, the MPLS-based VPNs are becoming increasingly popular. As defined by IETF, Resource Reservation Protocol with Traffic Engineering (RSVP-TE) and Label Distribution Protocol (LDP) are used to build LSPs in MPLS networks. Generally RSVP-TE builds the P2MP trees from the root to the leaves while LDP does in the opposite direction. However, RSVP-TE is the proper tree setup protocol for the scalable VPN multicast services, because it depends on the traffic engineered tree sharing. [14, 78-79; 15.]

2.3 Virtual Private LAN Service

The Virtual Private LAN Service (VPLS) is a service to provide multipoint-to-multipoint communication based on Ethernet across IP/MPLS networks. The synonyms of VPLS are Virtual Private Switched Network Service and Transparent LAN Service. VPLS meets the demands of broadcast or multipoint access among different networks. It connects together several geographically separated LANs to function as a single LAN across a packet

switched network. Here the provider network acts as a switch or bridge between two sites. By gluing sites with pseudo-wires, an Ethernet broadcast domain is shared among different sites. It is realized by adding network functions of MAC address learning, forwarding and flooding too. [17; 19.]

Figure 3 is an example of a simple VPLS network. As the figure shows, customer edge (CE) is the customer side device which is directly connected to the service provider device, while provider edge (PE) is the service provider side device which is directly connected to the customer device. CEs belonging to the same VPLS instance could communicate across the provider network, which acts as a single LAN. Over one shared provider network, more than one VPLS instances could be supported. However, CEs belonging to distinct VPLS instances do not have interaction. [19; 24.] In order to establish a fully meshed architecture, each pair of PEs participating in the same VPLS instance must have bidirectional pseudo-wire connection. In this way, the VPLS packet could be sent from ingress PE directly to egress PE, without the help of intermediate PE. [17; 20, 238.] VPLS packets are encapsulated and forwarded through tunnels which are used to implement the pseudo-wire. The tunnels could be MPLS or IP tunnels. [18; 20, 238.]

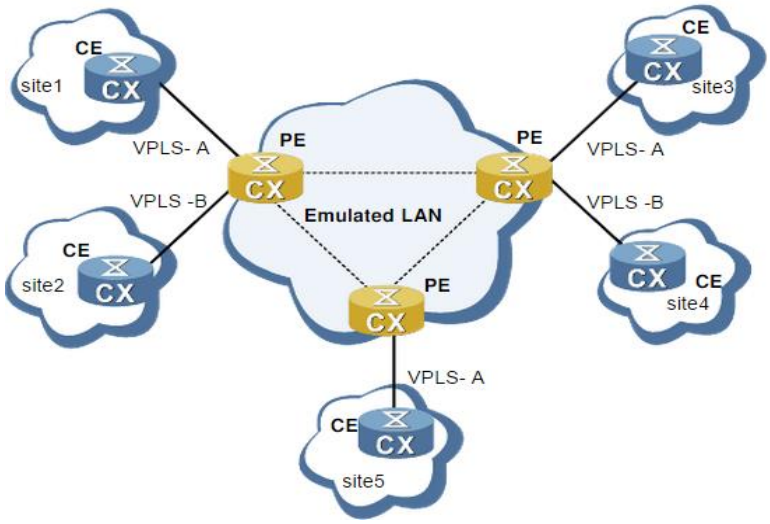

Figure 3. A simple VPLS network. Modified from “A novel distributed spanning tree protocol for provider provisioned VPLS networks” [24].

The process of finding other routers under the same VPLS or VPN is called auto-discovery. In addition, the setup and teardown of pseudo-wire connection is named signalling. There

are two protocols used to build VPLS full mesh structure: border gateway protocol (BGP) and label distribution protocol (LDP). [17; 18.] The VPLS control plane means the approach by which PEs interact for auto-discovery and signalling, while the VPLS data plane refers to the pseudo-wire where customer VPLS packets are sent between PEs [23].

There are several differences between BGP and LDP. With BGP, the PE could automatically detect all the other PEs in the same VPLS instance, and then establish the pseudo-wire connection to them [17]. However, with LDP, each PE device should be manually configured a VPLS instance and given all other PEs' addresses in the same VPLS. Then a LDP session has to be created between pair of PEs before the full mesh pseudo-wire connection is established. In this aspect, BGP has higher requirements to PEs than LDP. [18.] Additionally, the number of LDP sessions would become very large as the PE number increases. BGP solves this problem by utilizing the route reflector to effectively reduce the BGP session number. Moreover, with LDP, only one label is distributed to each PE if needed. However, BGP allocates a label block, which is considered as behaviour of wasting the label resources. Therefore, BGP and LDP are incorporated in the network covering large amount of nodes and area, with BGP method in the core network and LDP method in the access network. [22, 388; 23.]

As the network grows rapidly, more and more sites need to be linked together by VPLS. Thus, the scalability of VPLS becomes increasingly important. A new VPLS technology called hierarchical VPLS (HVPLS) came up. HVPLS uses multi-tier hierarchical architecture to implement a VPLS VPN, so that it is simplified to some extent by reducing the total number of pseudo-wire. HVPLS divides PEs into two types: U-PE and N-PE. U-PE refers to user-facing provider edge, which is responsible of forwarding the traffic from CEs to an N-PE node. N-PEs switch the customer data in L2 layer by means of bridging. Therefore, N-PEs have to learn customer MAC addresses got from all other N-PEs and U-PEs in the core network. In this way, the burden of U-PEs is released, but there are still a substantial number of pseudo-wires required to connect the N-PEs. And N-PEs have to learn a large number of MAC addresses as the customers grow, which would cause some problems. [21, 174; 22, 388.]

To improve the VPLS scalability even further, the provider backbone bridging (PBB) technique is incorporated in HVPLS with the MPLS access network. The U-PE is provided

with a PBB backbone edge bridge functionality, which encapsulates the customer packets with a PBB header and switches them to an N-PE. [21, 176.] Figure 4 is the scheme of HVPLS with PBB access network. As figure 4 shows, U-PE A does both MPLS and PBB encapsulations. The PBB header contains the backbone destination and source addresses. U-PE A forwards the packet to N-PE A. Then N-PE A does the lookup based on the backbone destination address and sends the packet on the correct pseudo-wire across the VPLS core. N-PE B receives the packet and performs the MAC address lookup, based on which it is sent to U-PE B. Finally U-PE B decapsulates both MPLS and PBB headers and forwards the packet to the correct customer node. [22, 389-390.]

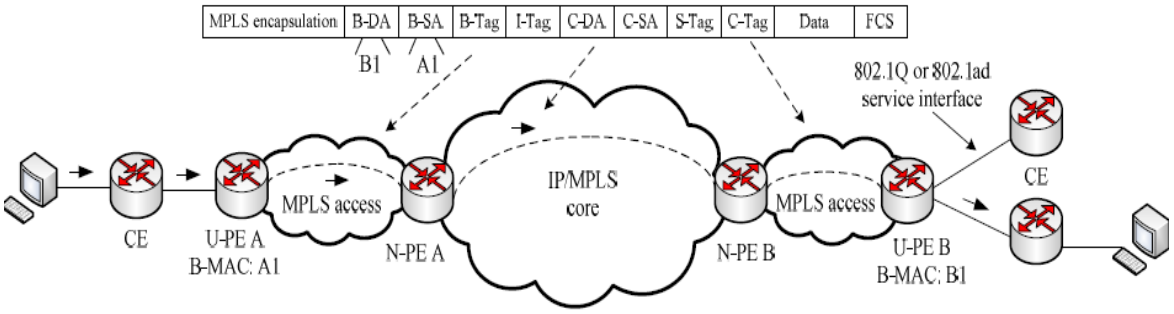

Figure 4. HVPLS with PBB access network. Copied from “Designs of PBB interoperating with H-VPLS based on MPLS networks” [22].

HVPLS with PBB access network has shown several advantages. First, N-PEs are required to learn the MAC addresses of U-PEs only, so that the number of MAC addresses stored in N-PEs could be significantly reduced. Second, the backbone address design improves the VPLS scalability since bridging is according to the backbone addresses rather than the huge amount of customer addresses. Third, the 24-bit I-SID space could support much more service instances than the 12-bit VLAN space, greatly contributing to the VPLS scalability. [21, 177; 22, 390.]

2.4 Ethernet VPN

2.4.1 Ethernet VPN Background

In the case of the Ethernet multipoint connecting requirement, the VPLS is usually deployed in an MPLS/IP network. Various L2VPN applications, such as the Ethernet

business service and company campus L2 transport, already exist. However, in recent years the Data Center Interconnect (DCI) application has been used widely in Ethernet multipoint L2VPNs. As data centers with better qualities become increasingly flexible to users, a new set of requirements appears, with higher speed, optimized resource utility and less cost. In order to achieve these, several functionalities should be supported by the DCI solution, such as error recovery and work continuity, data and virtual machine mobility, cloud and virtualization services. [25, 3; 26.]

In the scenario of DCI, current VPLS solution could not meet all the requirements alone. First, data centers require per-flow load balancing support. However, now VPLS provider edge dual-homing solutions include only per-VLAN scenarios, offering restricted load balancing support. VPLS could not address the challenging that one particular VLAN has very heavy data flow, which requires the manual administration to reallocate VLANs to particular PE. [25, 2.] Second, large data centers contain a big number of MAC addresses and VLANs to be stored in PEs. However, at this moment the number of PEs in the VPLS solution depends on the allowed number of pseudo-wires in the core network, which are normally some hundreds. Last, if any change of network topology occurs, the packet loss and downtime must be minimized by rapid convergence. [27; 28, 5.]

Nowadays, the EVPN family technologies include new generation Ethernet L2VPN solutions that address point-to-point service named as “E-LINE”, multipoint service name as “E-LAN” and rooted multipoint service named as “E-TREE”. All the three service types are under the same EVPN architecture. [26.] The technologies of EVPN and Provider Backbone Bridging EVPN (PBB-EVPN) belong to the “E-LAN” solution. The most significant difference between them and VPLS is that they utilize BGP as control plane to learn MAC addresses over the core, and to discover the VPN endpoints. [27.] In this way, EVPN introduces a novel model for L2VPN service delivery by separating and abstracting the data plane and control plane [28, 8].

There are three main building parts for EVPN and PBB-EVPN technologies: EVPN instance (EVI), Ethernet segment (ES) and BGP routers. Similar as the IP VPN Routing and Forwarding, EVI is equal to a VPN in a provider edge router. A bridge domain is linked to an EVI for forwarding traffic to the core network. There are several modes to map the

traffic to the bridge domain depending on the service actions, including multiple-to-one mapping, selective bundling and one-to-one mapping. [25, 4; 29.]

ES means the access network or device connections. Ethernet bundle is the access interface that connects CE to PEs. Ethernet segment identifier (ESI) is the ID of the Ethernet segment. Due to the requirements of access redundancy and multi-homing, a customer network or device could be linked to more than one PE connected to the same MPLS core. A single-homed network (SHN) / device (SHD) and a multi-homed network (MHN) / device (MHD) are the four cases of ES. [30.] In MHDs, there are all-active balancing mode and single-active balancing mode of operation. The former mode supports per-flow load balancing for MHDs while the latter supports per-VLAN load balancing for MHDs. [31.] Figure 5 is a graphic explanation of the two modes on a dual home device.

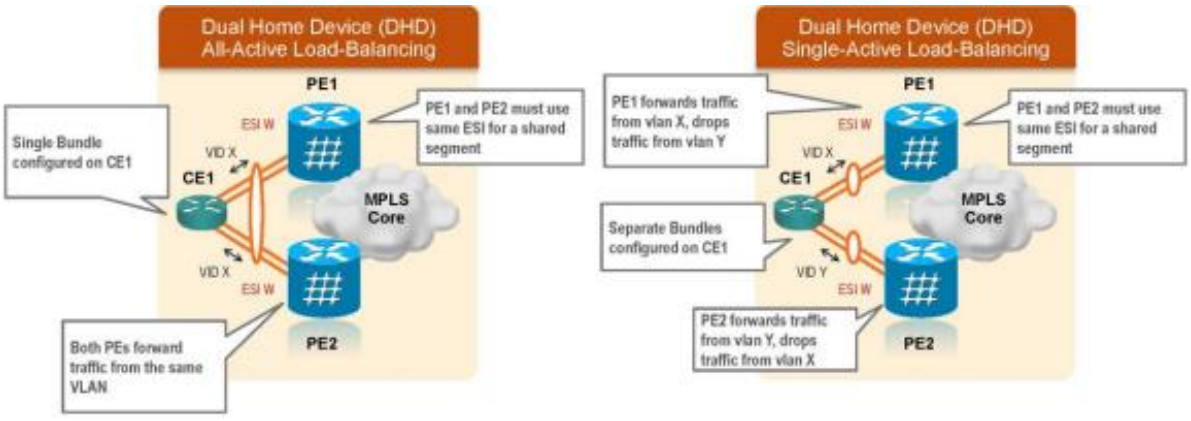

Figure 5. All-active and single-active balancing modes of EVPN.
Copied from “Ethernet VPN and provider backbone bridging-EVPN” [25, 4].

As figure 5 shows, in the all-active load balancing mode, the access device is linked to two PEs through the same Ethernet bundle. The CE could forward and receive data of the same VLAN from all the PEs belonging to the same ES. However, in the single-active load balancing mode, the access device is connected to two PEs via two separated Ethernet bundles. The VLAN forwarding tasks is separated and assigned to individual PE with one given VLAN responsibility. In figure 5, PE1 is only responsible for VLAN X while PE2 only for VLAN Y. Through data plane learning, the CE could know the mapping of VLANs to Ethernet bundles. [25, 4; 28, 10.]

Compared to only data plane learning in the VPLS solution, EVPN and PBB-EVPN technologies allow MAC address signalling and learning by BGP over the core network. The multi-protocol BGP (MP-BGP) control plane makes PEs to publish and learn prefixes identifying ES and MAC addresses. In addition, by combining MPLS data plane, the BGP routers can signal MPLS labels as well. [30.] As a result, pseudo-wires are not needed in EVPN, since there is no need to signal different P2P pseudo-wire VC labels for each PE in the network. Instead, MPLS labels indicate multipoint-to-point (MP2P) LSPs that are signalled by other PEs in the same VPN. From this aspect, EVPN technologies integrate L2VPN and L3VPN to realize layer2 and layer3 services integration. [29; 31.]

2.4.2 Ethernet VPN Operations

In an all-active multi-homed case, PEs linked to the same ESI could discover each other via auto discovery mechanism. A designated forwarder (DF) should be selected to send a broadcast, unknown unicast and multicast (BUM) data flow to the ES. Only one copy of the BUM flow is allowed to the CE from the DF. Non-DF PEs must block BUM traffic to CE. [28, 14; 32.] The split horizon mechanism is utilized to make sure that BUM data flow from one ESI would not be looped back to itself. Similarly, the BUM flow received from the core could not be sent back to the core. The split horizon label is used to identify the source ES of BUM data flow, and the egress PEs use the label to filter away the packets sent to the ES indicated by the label. [28, 15; 30.]

Besides the redundancy group membership discovery, the PE also discovers the remote ESIs and whether they are all-active or single-active load balancing mode. Normally, PE advertises not only MAC addresses and its own ESI, but also connectivity to remote ESIs. When a link failure happens in one Ethernet bundle, the PE simply withdraws the route for the ESI. Then rapid convergence is triggered and remote ESIs do MAC mass withdraw by deleting the failed PE from the route for all MAC addresses related to the failed ESI. [25, 5.] An interesting case is that a MAC address might move from one ESI to another. The PE cannot notice the moved MAC address from its ESI and delete its MAC route, since it is learnt via data plane. At the same time, another PE where the MAC address moves to would send a new MAC route. A MAC mobility sequence number is generated and advertised together with the MAC route, so that remote PEs could choose the biggest mobility sequence number MAC route. [28, 18; 31.]

Figure 6 is an example of control plane advertisement and learning over the MPLS core. As it shows, when a customer packet with source MAC address M1 is received by PE1, local data plane learning happens. Then control plane advertises the MAC route of M1 to PE2, PE3 and PE4. In the case of segment failure on the Ethernet bundle connecting CE1 to PE1, PE1 would remove M1 MAC entry in the advertisement and all other PEs in the MPLS core would delete PE1 from the M1 MAC route. [25, 6.]

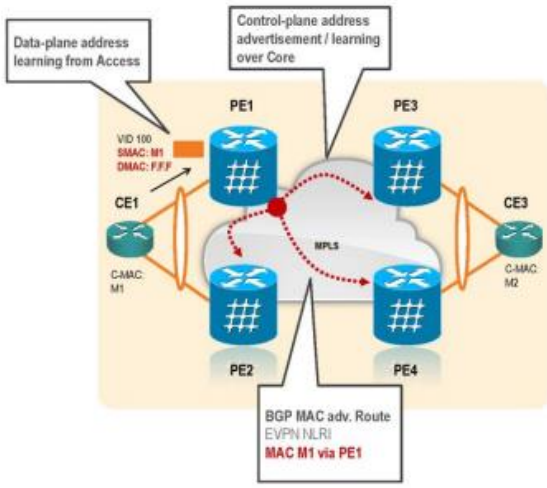

Figure 6. An example of control plane advertisement and learning in EVPN. Copied from “Ethernet VPN and provider backbone bridging-EVPN” [25, 6].

The PBB-EVPN operation integrates the EVPN and PBB functionalities, providing several advantages over an EVPN solution. For instance, it has lower requirements for the scale of the control plane, and handles the MAC move event faster. [25, 8.]

2.4.3 Ethernet VPN Applications

The EVPN technology provides L2 and L3 services integration through one interface and one VLAN. Figure 7 is a graphic summary of layer 2 and layer 3 services provided by EVPN technology. As it indicates, without the combination of several VPN protocols, EVPN could offer both services alone. A customer could choose an all-active or single-active load balancing mode to link PE with CE according to his/her needs. Basically, any core network could run EVPN. For instance, when MPLS is unavailable or not desired in the core, EVPN is run above a virtual extensible LAN (VXLAN) data plane in a simple IP

core. However, when MPLS is available, the original EVPN-MPLS solution will be adopted. [29; 32.]

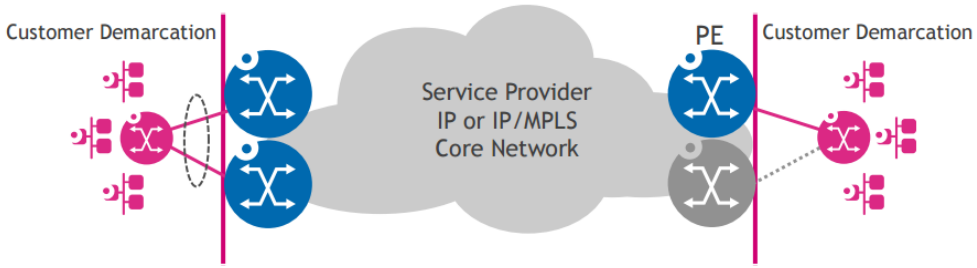

Figure 7. EVPN layer-2 and layer-3 services.
Copied from “Ethernet VPN for integrated layer 2-3 services” [29].

Another EVPN application is the scalable L2 or L3 DCI services for virtualized data centers. When an MAC address moves from one data center to another, each PE at the local data center gateway optimizes the routing and the IP/MAC mobility is signalled by a control plane. As a result, L2 bridging and L3 routing is integrated well in one service. [33.]

3 Methods and Materials

3.1 Technical Materials

The thesis work is carried out in Ericsson, Finland, and the hardware resources are provided by Ericsson, Finland. The next generation network processing unit and the testing equipment are purchased from Ericsson’s chip vendor, and the programmer’s reference guide and the architecture guide of the next generation chip are provided by the chip vendor. Workstation, servers, unified test bed, traffic generator and network services are provided by Ericsson, Finland.

The software resources are partly provided by Ericsson and partly downloaded from the Internet. CINT is used as the command line C interpreter to apply the code on the NPU. The latest software development kit (SDK) of the next generation chip is provided by the chip vendor. All other general technical materials are freely downloaded from the Internet.

3.2 Intangible Materials and Financial Cost

The thesis work is carried out by myself independently. Most of the related intangible materials and financial cost are covered by Ericsson, Finland. Instructors from both Ericsson and the Helsinki Metropolia University of Applied Sciences provide necessary technical support, and a language advisor from the Helsinki Metropolia University of Applied Sciences provides necessary language guidance.

3.3 Technologies and Methods Applied

The methodology of comparison is mainly used in the thesis work. Emerging in 2007, the VPLS is still widely used as an Ethernet L2VPN solution in the telecommunication field nowadays. The next generation NPU offers an opportunity to implement the EVPN feature to fulfil new sets of requirements that are not readily addressable by the current VPLS solution. The comparison of the VPLS and EVPN technologies is mainly made from the aspects of address learning, service types, flow optimization, resiliency and provisioning. Additionally, the known unicast packet flow in EVPN is used as a comparison case to VPLS and verified in the unified test bed.

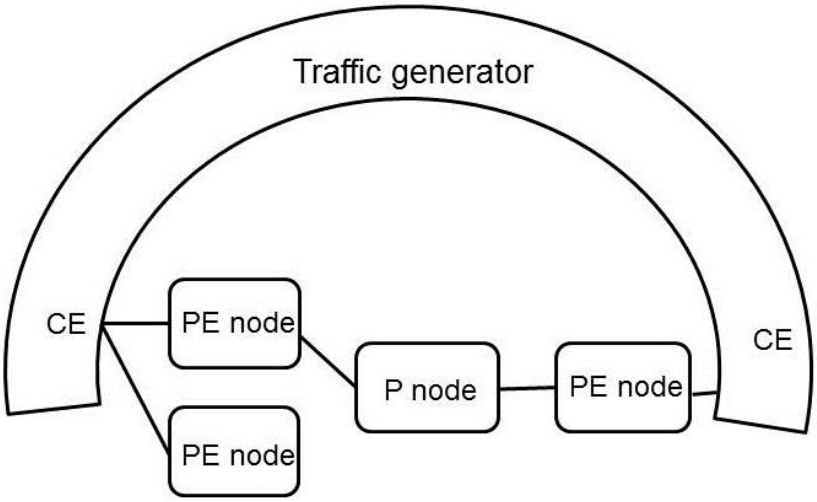

Figure 8. Test bed structure used in the EVPN data flow testing.

An EVPN topology is generated and a data flow scenario is designed. Figure 8 is the test bed structure used in the data flow testing of EVPN. As it shows, traffic sending and receiving is produced and verified by the traffic generator. A next generation NPU equipped test machine is referred to as a node. Some nodes simulate the provider edge (PE) devices in EVPN and some simulate the provider (P) devices. Since the customer edge (CE) devices send and receive packets in this scenario, the traffic generator simulates CE devices. Traffic going through each node is monitored by the debugging tools offered together with the NPU package.

4 Results and Discussion

4.1 Address Learning of VPLS and EVPN

In the VPLS, the layer 2 and layer 3 reachability information cannot be advertised and shared by the control plane like in VPNs based on BGP. That means the MAC address knowledge could only be learned through the standard bridge learning mode. Figure 9 is a typical VPLS topology and an example of a traffic flow. The scenario in figure 9 is a packet containing the source MAC address of CE1 and destination address of CE3 arrives at PE3 on the PE1-PE3 pseudo-wire port. At the same time, PE3 does not have the MAC entry of CE1 in its MAC table. Then PE3 associates CE1 MAC address with PE1-PE3 pseudo-wire port and stores it in its MAC table. Therefore, if later a packet containing the destination address of CE1 arrives at PE3, it will look up the MAC table and forward it to the PE1-PE3 pseudo-wire port correctly.

Similarly, when a packet containing the source MAC address of a device in Site 3 network arrives at PE3 on the attachment circuit (AC) port, PE3 does not have the source MAC entry. It will associate the source MAC address with the AC port and store it in its MAC table. Later, when packets with the destination MAC address of that device arrive at PE3, it will make the right forwarding decision.

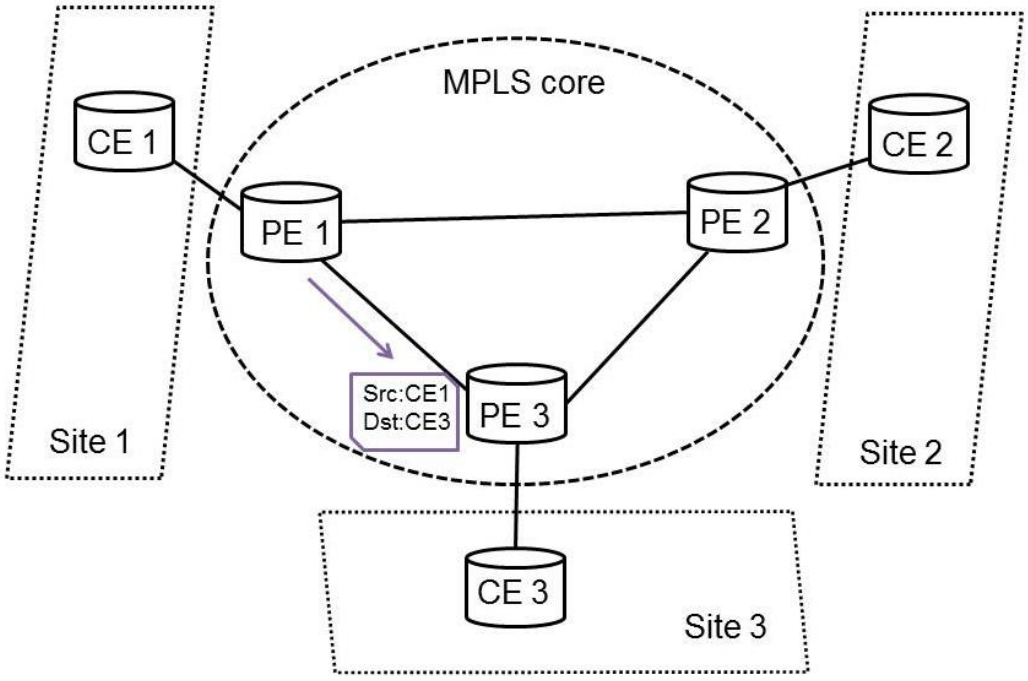

Figure 9. A typical VPLS topology and an example of traffic flow.

The standard bridge learning mode has a significant drawback. Here I take the above example again. If the PE3 MAC table does not have a CE3 MAC entry when the indicated packet arrives, the packet will be considered an unknown unicast packet. If the administrative policy allows, it will then be flooded over all the attachment circuits and pseudo-wires except the PE1-PE3 pseudo-wire where the packet comes from. The decision will be changed until the PE3 MAC table has a new entry for the CE3 MAC address. If this occurs in the case of a large-scale network frequently, a huge number of unknown unicast packets will waste much network resources and cause an efficiency problem.

However, EVPN adopts a combination of data plane learning and control plane learning [34]. In EVPN, PE learns the CEs that directly connect to it by data plane learning, which is also called local learning. It means that a PE must be able to learn the address knowledge of customer networks using the standard Ethernet learning procedures, like the way applied in VPLS. The supported packet types could be, for instance, ARP request for its own or peer's MAC address, or DHCP request. In EVPN, MAC mobility is supported as well. It means that a MAC address belonging to one Ethernet segment could move to another segment, with the two segments directly connected to the same or different PEs. If

the MAC movement happens frequently between the same two Ethernet segments, the MAC mobility extended community attribute would contain a sequence number. All the PEs making forwarding decision to the moved MAC address always choose the route with the highest number of the sequence number. As a result, the packet is forwarded to the latest moved Ethernet segment clearly.

In EVPN, a PE can also learn the MAC addresses of other Ethernet segments that do not directly connect to itself. This is called remote learning, which is realized by MAC/IP address advertisement through multiprotocol-BGP (MP-BGP) distribution. MAC/IP address advertisement route is contained in the EVPN network layer reachability information (NLRI) packet. [35.] Figure 10 is the structure of the EVPN NLRI. As it shows, the first byte indicates the route type stated in the route type specific field. There are four route types in total in EVPN NLRI: Ethernet auto-discovery (A-D) route, MAC/IP advertisement route, Ethernet segment route and inclusive multicast Ethernet tag route. The second byte indicates the data length of the route type specific field. The last part of EVPN NLRI specifies the detailed route information, which definitely indicates the corresponding route type simultaneously. The length of this field varies depending on different route types.

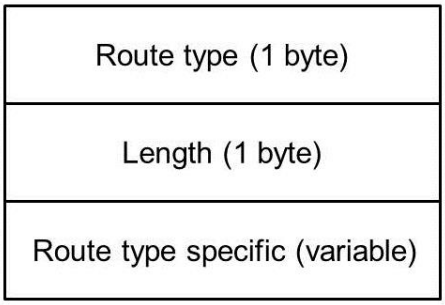

Figure 10. Structure of EVPN network layer reachability information.
Modified from “BGP MPLS based Ethernet VPN” [35].

Figure 11 is the structure of a MAC/IP advertisement route specified in the EVPN NLRI. The first field route distinguisher (RD) is unique to the MAC-VRF which is advertising the reachability information. The RD is used to specify a certain MAC-VRF among many of those on one PE. In RD, the IP address of the PE and the VLAN-ID is specified to indicate a certain MAC-VRF. The second field is the Ethernet segment identifier that indicates one certain ES. The 10-byte ESI field contains an one-byte ESI type subfield and a 9-byte ESI value subfield. The third field is the Ethernet tag identifier which includes a 12-bit or 24-bit

identifier that specifies a certain broadcast domain in an EVPN instance. It is called VLAN ID (VID). In cases of VLAN based service interface and VLAN bundle service interface, the Ethernet tag in route is set to zero. However in the case of VLAN-aware bundle service interface, the Ethernet tag identifier is set to a non-zero value, since there are more than one MAC tables under one MAC-VRF. Each VLAN-ID corresponds to one broadcast domain. If in a certain VLAN, the VLAN-ID varies according to different CEs, the provider's VLAN-ID will be filled in the field. [35.]

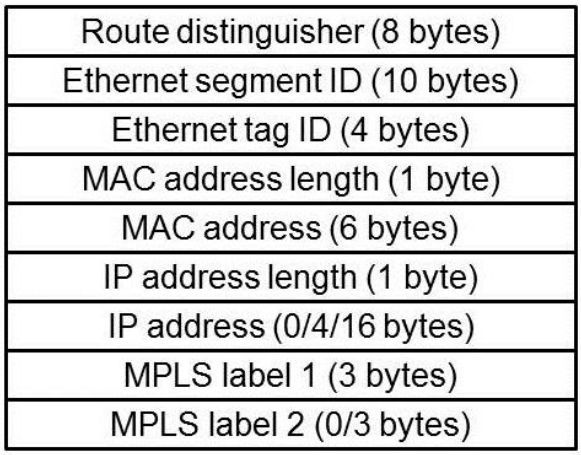

Figure 11. Structure of MAC/IP advertisement route of EVPN.
Modified from "BGP MPLS based Ethernet VPN" [35].

The MAC address field is compulsory while the IP address field is optional [34]. The IP address field supports both 4-byte IPv4 address format and 16-byte IPv6 address format. Advertising both MAC and IP reachability information is the way in which EVPN is able to integrate layer-2 and layer-3 service. Both MAC address length and IP address length fields are in bits. From the IP address length field, either IPv4 or IPv6 address is revealed.

The MPLS label 1 field is compulsory and contains a 24-bit value. The 20-bit MPLS label value fits into the front 20 bits of the field. There are four options for the advertising PE to assign the MPLS label in the route. First, the MPLS label could be unique to a certain MAC address that the PE advertises in a certain EVPN instance. That means it is used by the advertising PE to forward the received unicast packet to correct CE based on the destination MAC address. Second, the MPLS label is unique to ESI and VLAN combination. The above two options allow the PE to forward the recevied packets to the

CE network solely based on the MPLS label without performing any MAC address lookup. Third, the MPLS label is unique to MAC-VRF and VLAN combination in the case of VLAN-aware bundle service interface. The last option is that the MPLS label is unique to MAC-VRF in the cases of VLAN-based service interface and VLAN bundle service interface. [34.] These two options require the advertising PE to look up the corresponding MAC table associated with the MPLS label to find the entry of the destination MAC address and make a forwarding decision.

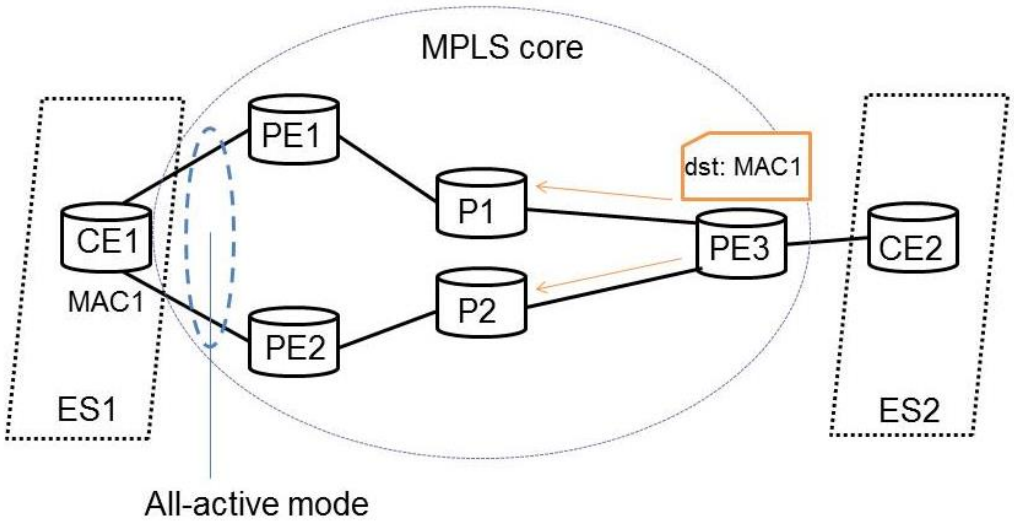

Figure 12. A typical EVPN topology and a proposed scenario.

Figure 12 is a typical EVPN topology and a proposed scenario. As it shows, PE1 and PE2 are connected to the multi-homed ES1. And EVPN all-active redundancy mode is applied. MAC1 is the address of some device inside ES1 network. PE1 learns MAC1 by local learning. But PE2 does not. Then if PE3 receives the MAC/IP advertisement route from PE1 and Ethernet auto-discovery per Ethernet segment routes and Ethernet auto-discovery per EVPN instance routes from both PE1 and PE2, PE3 will forward packets with MAC1 as the destination MAC address to both PE1 and PE2, because PE3 learns from the auto-discovery route that PE2 connects directly to the Ethernet segment that MAC1 locates. If either PE1 or PE2 withdraws the Ethernet auto-discovery per Ethernet segment routes, PE3 will forward the packets to the other one. If PE1 withdraws the MAC1 MAC/IP advertisement route, PE3 will consider the packets as unknown unicast packets. Another scenario is that, if PE1 withdraws the MAC1 MAC/IP advertisement route and PE2 advertises MAC1 MAC/IP advertisement route, PE3 will forward the packets to both

PE1 and PE2, since PE3 learns from the auto-discovery route that PE1 connects directly to the MAC1 segment.

4.2 Flow-based Load Balancing of EVPN

As stated in chapter 2, there are two redundancy modes that are applied in a multi-homed device in the EVPN, single-active and all-active redundancy modes. If the remote PE receives the Ethernet auto-discovery per Ethernet segment route whose ESI label extended community has the flag of single-active set to one, the PE will know that the advertised ESI acts in single-active redundancy mode. Then the remote PE would consider the PE advertising the MAC/IP advertisement route as the primary PE, which is the designated forwarder of the advertised ESI at the same time. If the remote PE receives the Ethernet auto-discovery per Ethernet segment routes for the same ESI from other PEs, it will consider those PEs as the backup PEs for the announced ESI. [35.] Therefore, if there is a link failure happening on the primary path, the backup paths would be used to forward the traffic to the ESI from the remote PE.

Taking the topology in figure 12 as an example, PE1 and PE2 connect to ES1 via single-active redundancy mode here. And PE1 is the DF of the segment. When PE3 receives the MAC/IP advertisement route of MAC1 from only PE1 and the Ethernet auto-discovery routes that indicate the direct link to ES1 from both PE1 and PE2, it will consider that PE1 as the primary PE while PE2 as the backup PE for MAC1. Link failures between ES1 and PE1 would trigger the withdrawal of Ethernet auto-discovery route from PE1 and subsequent MAC/IP advertisement route of MAC1 from PE1. Then PE3 would update its MAC entry for MAC1 to point to the backup PE, which is PE2. At the same time, PE2 learns MAC1 through local learning and send the MAC/IP advertisement route of MAC1 to PE3. In this way, there is no flooding happening in case of network failure, so that the network resource is not wasted and the data transfer efficiency increases. This is an advantage of EVPN compared to VPLS and other L2VPN technologies.

If multiple backup PEs exist for one Ethernet segment, the remote PE does not know which backup to use. Therefore, if the administrative police permits, flooding to all other

directly connected PEs of the ESI occurs. As a result, EVPN generates an efficient way to overcome fail-over events and makes a switch-over quickly.

In case of all-active redundancy mode in figure 12 topology, PE3 would know the mode type from the Ethernet auto-discovery per Ethernet segment route whose ESI label extended community has the flag of single-active set to zero. PE3 will send the packets with MAC1 as the destination MAC address to both PE1 and PE2, even though PE2 does not send the MAC/IP advertisement route of MAC1 to PE3. When constructing the MPLS label stack, PE3 makes two MPLS next hops to PE1 and PE2 respectively. To PE1, the MPLS label advertised by PE1 for MAC1 is added first, followed by the MPLS LSP stack to get to PE1. To PE2, the MPLS label in the Ethernet auto-discovery route advertised by PE2 for ES1 is added first, followed by the MPLS LSP stack to get to PE2. There are two ways for PE3 to balance the IP traffic to MAC1. One way to select one of the next hops is according to the source MAC address, while another way is to use a hash algorithm to map the traffic to either of the two next hops.

The feature of flow-based load balancing is missing in the VPLS technology. In the EVPN, it greatly optimizes the network efficiency and separates heavy traffic into many directions, especially in large-scale networks. Moreover, all the PEs are utilized to forward traffic to Ethernet segments, alleviating the load for the DF PE, by applying all-active redundancy mode. Since one PE is the DF of one segment and VLAN combination, while another PE is the DF of another segment and VLAN combination, all the links between ES and core network should share more or less equal amount of traffic load. Additionally EVPN fast re-routing is guaranteed by the flow-based load balancing.

4.3 Integrated Services Provided by EVPN

As stated in section 4.1, the MAC address field is compulsory and the IP address field is optional in EVPN MAC/IP advertisement route. If the IP address information is advertised along with the MAC address, it will reduced the amount of address resolution protocol (ARP) request and neighbour discovery (ND) messages across the MPLS core. If there are multiple IP addresses associated with one MAC address, they will be separated into different MAC/IP advertisement routes to be advertised to remote PEs [34]. For instance,

an IPv4 address and an IPv6 address could be associated to the same MAC address. And the MAC/IP advertisement route support both address formats. This is another example in EVPN to minimize unnecessary flooding messages and optimize the network efficiency.

In EVPN, a MAC/IP advertisement route with only MAC information and the one with both MAC and IP information are independent to each other. One example is, if the advertising PE withdraws the route with both MAC and IP information caused by the ARP timeout event, the route with only MAC information is not affected at all. The MAC entries still exist in the MAC-VRF table of the advertising PE and the receiving PE. But the ARP entry of the MAC in the receiving PE is deleted once the withdrawal happens. [35.]

Normally, if a CE sends an ARP request to the receiving PE about a device belonging to another segment which is not directly connected to the receiving PE, the PE can act as an ARP proxy and respond to the request by looking up its ARP table [35]. Therefore, ARP request and response about one device can be done in the remote PEs and their segments, without having to send the ARP request and response back and forth. This is one method that EVPN utilizes to integrate layer 2 and layer 3 services.

4.4 Programming and Testing on Next Generation NPU

Network processing unit plays the most important role in computer networking. It possesses similar features as a normal CPU, but works mainly in networking equipment and products. The next generation NPU that used in this thesis work is software programmable. The CINT is used as a C interpreter in the coding environment. Basically the programming is based on the hardware SDK provided by the chip vendor, while the testing is performed by sending and receiving traffic through an emulated MPLS core network.

4.4.1 Proposed EVPN Topology and Scenario

Figure 13 is the EVPN topology used in the prototyping and testing. As it shows, PE1 and PE2 connect directly to Ethernet segment 1. All-active redundancy mode is applied by PE1 and PE2 in the connection to CE1. PE3 attaches to Ethernet segment 2 and CE2

directly. PE3 connects to PE1 and PE2 via P. The MAC address of CE1 is 00:00:00:00:00:11 and CE2 is 00:00:00:00:00:22. A packet with source address of CE2 and destination address of CE1 arrives at PE3. PE3 forwards the packet to P device. Then P device forwards the packet to both PE1 and PE2. Finally CE1 receives the packet.

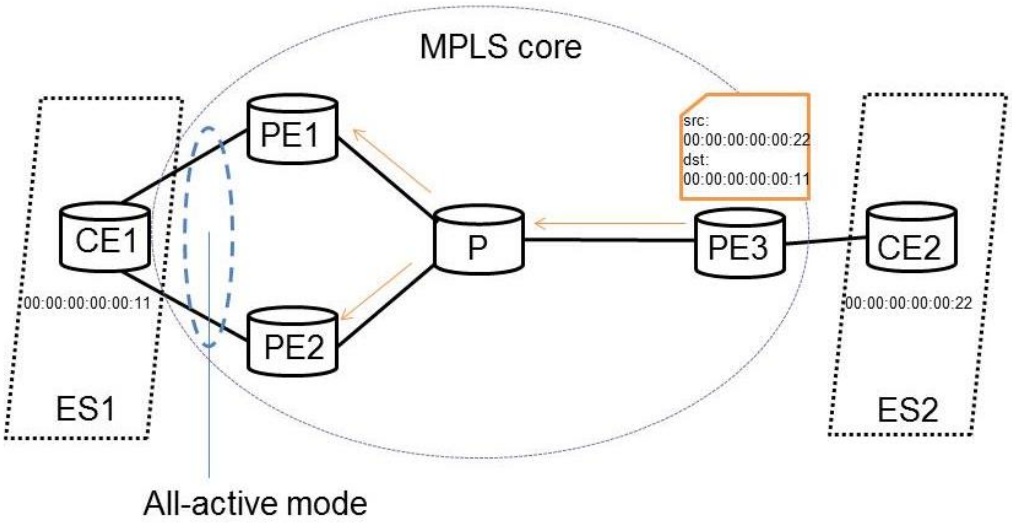

Figure 13. EVPN topology for the prototyping and testing.

The EVPN topology indicated in Figure 13 contains the fundamental components of an EVPN network. In a real situation, a more complicated network topology may exist, which will be discussed later in chapter 4.

4.4.2 Prototyping on Next Generation NPU

As the ingress PE to forward the known unicast packets, PE3 plays an important role in this scenario. In a real situation, PE3 should learn the MAC address of CE1 via MP-BGP distributed by PE1. However, in the testing environment, CE1 MAC is statically configured in PE3. Meanwhile, the EVPN instance, layer-2, layer-3, MPLS tunneling objects and nexthop object should be created on PE3 hardware. The order to program on PE3 NPU is the following:

1. Define a structure that contains all the hardware objects needed in the NPU, and define a structure instance and initialize all the member variables;
2. Create an EVPN instance on the hardware;

3. Perform layer-2 settings on the hardware, including layer-2 port and VLAN settings;
4. Create an attachment circuit ingress layer-2 logical interface for CE2;
5. Create layer-3 ingress routing interface for the layer-2 logical interface and layer-3 egress routing interface for P device in the MPLS core;
6. Create an egress tunnel pointing to the above egress routing interface;
7. Create two nexthop objects, one points to PE1, and the other one points to PE2;
8. Create static MAC table entry for CE1 MAC address, with the destination port pointing to the above egress tunnel.

As the connecting device of different PEs in the MPLS core, P is unaware of the EVPN instance and any information in the customer networks. It is only responsible for parsing the MPLS LSP label stack and forward the packets to the correct tunnel. In this case, if P receives the packets with PE3-PE1 LSP label on top of the label stack, it will forward them to PE1; if PE3-PE2 LSP label, it will forward to PE2. In real situation, provider devices may perform label pop, push and swap actions on the label stack in order to forward packets to the right destination. But in the testing environment, due to limited amount of devices in the unified test bed, only one provider device is designed in the MPLS core. The order to program on P device NPU is the following:

1. Make layer-2 settings for the incoming packets on the NPU, including layer-2 port and VLAN settings;
2. Make layer-2 settings for the outgoing packets on the NPU, including layer-2 port and VLAN settings;
3. Create layer-3 ingress routing interface for the incoming MPLS routing packets;
4. Create layer-3 egress routing interface for the outgoing MPLS routing packets;
5. Create an egress tunnel pointing to the egress routing interface;
6. Create two nexthop objects, for PE1 and PE2 respectively;
7. Add switch entry to the incoming label map (ILM) table on the NPU.

As the egress PEs for the known unicast packets, PE1 and PE2 should terminate all the MPLS labels and forward the packets to the attachment circuit leading to CE1. It is realized by the ingress termination tunnel. After MPLS label termination, the heading of the packets are restored to the original format when they first entered into the MPLS core network. And PE1 and PE2 forward the packets to the correct node by adding new layer-2

encapsulation and possible VLAN translation according to the destination MAC address. The order to program on PE1 and PE2 NPU is the following:

1. Create an EVPN instance on the chip;
2. Create an attachment circuit ingress layer-2 logical interface for P;
3. Create an attachment circuit egress layer-2 logical interface for CE1;
4. Create an ingress termination tunnel for PE3-PE1 or PE3-PE2 LSP label;
5. Create an ingress termination tunnel for EVPN label.

4.4.3 Testing on Next Generation NPU

Packets with proper layer-2 encapsulation are generated by the traffic generator and sent out from the correct port to the MPLS core. Traffic going through PEs and P device are monitored by the hardware debug tools. The results show that all devices are receiving correct packets with proper headings. The results also show that the traffic generator receives the final packets to the receiving port. Therefore, the layer-2 traffic is generated, sent and received correctly based on the proposed EVPN topology and scenario.

4.4.4 Limitations of the Study and Future Improvements

EVPN is a very new technology. The initiative RFC related to EVPN was just standardized by IETF in February 2015. NPU vendors were just starting to embed the new feature on their hardware. So there may be certain NPU SDK bugs that have not been disclosed in this study. This study has been trying to find the EVPN availability and providing the basic prototyping of EVPN on the next generation NPU. There are some limitations.

First, in our current testing environment, the number of devices equipped with the next generation NPU was limited. So the number of provider devices in the core network was limited to one. One provider device is enough to make the simple topology work, as long as it directly connects to all other PEs. In the stage of implementation of EVPN feature on Router 6000 series, a larger scale of testing environment is required.

Second, MP-BGP distributed MAC/IP advertisement route in EVPN was not included in the prototyping, because it was out of the scope of the study. Instead, statically configuring

MAC address was applied in the prototyping and testing. However, in a real EVPN scenario, MP-BGP is necessary to distribute different kinds of routes to the remote PEs, including MAC/IP advertisement route and Ethernet auto-discovery route. These should be considered and improved in the future work.

Third, only known unicast traffic was prototyped and tested in the study. In a real situation, broadcast, multicast and unknown unicast traffic all exist. And the prototyping on the NPU would be different due to different types of traffic and administrative policies applied on the network. Therefore, more traffic scenarios could be generated and studied in the future, for instance, prototyping and testing on the ingress PE NPU and egress PE NPU for BUM traffic.

5 Conclusions

The thesis work was performed during the software development period of Ericsson Router 6000 Series. Since the new router family products are required to be competitive and up-to-date in the market, the new generation networking and communication technologies are strongly recommended to be implemented on them. The goals of the thesis work were to compare VPLS and EVPN technologies, to explore the advantages of an EVPN solution, to discover possible EVPN availability on the next generation NPU, and to provide pilot research results and references for the future implementation of EVPN on Ericsson Router 6000 Series.

In this study, several results were achieved. First, VPLS and EVPN technologies were compared from the perspective of address learning. The results show that EVPN utilizes not only MP-BGP to distribute address information to the remote PEs, but also data plane learning for the local attached network. This is superior to the auto-discovery and signaling approaches in the VPLS technology, which require complicated PW establishment and recognition.

Second, the comparison of VPLS and EVPN were performed from the aspect of flow optimization. The results show that the flow-based load balancing feature exists in EVPN

but not VPLS. It significantly increases the network resiliency and efficiency by separating the heavy traffic and utilizing every PE to the maximum extent. Also, the mechanism of primary path and backup path switch-over in the single-active redundancy mode improves the network stability and security in EVPN.

Third, a comparison was performed in the services that VPLS and EVPN could provide. The results show that EVPN has the advantages of IP VPN and could integrate layer-2 and layer-3 services in the same interface, while VPLS provides layer-2 service only. In the EVPN, both MAC and IP information are learned and distributed through the core. Moreover the layer-3 information is optional to be distributed. Therefore, the service providers are free to apply L3VPN on top of L2VPN. However, VPLS distributes only layer-2 information among different PEs in the same VPLS instance. Thus it is impossible to realize L3VPN functionalities in VPLS.

Fourth, prototyping and testing were performed on the next generation NPU. The results show that it is possible for the NPU to support the EVPN feature. The generated code on different network devices upon the proposed EVPN topology could be references for the future implementation of EVPN on the router family products.

Overall, the thesis work was successful and achieved all the goals. As stated above, several limitations still exist in the study, which could be studied and improved further. First, in the future, the testing environment for the EVPN feature could be enlarged to enable the building of EVPN topologies that are close to a real situation. Second, in the next step, MP-BGP involved route advertisement and distribution could be prototyped and tested on the same NPU as well. Also different kinds of routes could be tried. Third, different kinds of traffic, other than the known unicast traffic, could be prototyped and tested on the same NPU. At the same time, more complicated topologies and scenarios would be designed and investigated further.

References

1. Ericsson SSR 8000 family [online]. Ericsson official website.
   URL: http://www.ericsson.com/ourportfolio/products/ssr-8000-family.
   Accessed 18 February 2015.

2. Ericsson SSR 8000 family of smart services routers [online]. Ericsson official website; June 2012.
   URL: http://archive.ericsson.net/service/internet/picov/get?DocNo=1/28701-FGB101989.
   Accessed 18 February 2015.

3. Router 6000 Series [online]. Ericsson official website.
   URL: http://www.ericsson.com/mwc2015/launches/router-6000-series.
   Accessed 8 March 2015.

4. Reuven Cohen, Technion. On the establishment of an access VPN in broadband access networks. IEEE Communications Magazine; February 2003: pp.156-163.

5. Robert Friend. Making the gigabit IPsec VPN architecture secure. Computer; June 2004: pp.54-60.

6. Rami Rosen. Creating VPNs with IPsec and SSL/TLS [online]. Linux Journal; 1 January 2008.
   URL: http://www.linuxjournal.com/article/9916?page=0,0.
   Accessed 20 February 2015.

7. Layer two tunnelling protocol “L2TP” [online]. IETF RFC 2661; August 1999.
   URL: http://tools.ietf.org/html/rfc2661#section-1.0.
   Accessed 20 February 2015.

8. Layer two tunnelling protocol (L2TPv3) [online]. IETF RFC 3931; March 2005.
   URL: http://tools.ietf.org/html/rfc3931.
   Accessed 25 February 2015.

9. Securing L2TP using IPsec [online]. IETF RFC 3193; November 2001.
   URL: https://tools.ietf.org/html/rfc3193.
   Accessed 25 February 2015.

10. OpenVPN security overview [online]. OpenVPN official website.
    URL: http://openvpn.net/index.php/open-source/documentation/security-overview.html.
    Accessed 8 March 2015.

11. George Swallow, Cisco Systems. MPLS advantages for traffic engineering. IEEE Communications Magazine; December 1999: pp.54-57.

12. Luc De Ghein. MPLS Fundamentals. Cisco Systems; December 2006: pp.249–326.

13. Daniel O Awduche. MPLS and traffic engineering in IP networks. IEEE Communications Magazine; December 1999: pp.42-47.

14. Isaias Martinez-Yelmo, David Larrabeiti. Multicast traffic aggregation in MPLS-based VPN networks. IEEE Communications Magazine; October 2007: pp.78-85.

15. Extensions to RSVP-TE for P2MP TE LSPs [online]. IETF RFC 4875; May 2007.
URL: http://tools.ietf.org/html/rfc4875.
Accessed 12 March 2015.

16. Howard Green. OpenFlowMPLS [online]. OpenFlow website.
URL: http://archive.openflow.org/wk/index.php/OpenFlowMPLS.
Accessed 12 March 2015.

17. VPLS using BGP for auto-discovery and signaling [online]. IETF RFC 4761; January 2007.
URL: http://tools.ietf.org/html/rfc4761.
Accessed 12 March 2015.

18. VPLS using LDP signaling [online]. IETF RFC 4762; January 2007.
URL: http://tools.ietf.org/html/rfc4762.
Accessed 12 March 2015.

19. Itsik Hen, Naama Yehieli. VPLS [online]. RAD tutorial; 2006.
URL: http://www2.rad.com/networks/2006/vpls/main.htm.
Accessed 12 March 2015.

20. Giuseppe Di Battista, Massimo Rimondini. Monitoring the status of MPLS VPN and VPLS based on BGP signaling information. IEEE Network Operations and Management Symposium (NOMS); 2012: pp.237-244.

21. Lu Feng, Xu Lei. Power data network VPN deployment based on PBB and H-VPLS. Second Pacific-Asia Conference on Circuits, Communications and System (PACCS); 2010: pp.174-177.

22. Weijia Zhu. Designs of PBB interoperating with H-VPLS Based on MPLS networks. Second International Conference on Future Networks; 2010: pp.388-390.

23. Husam Awadalla, Fibernet Bespoke Networks. Wide area Ethernet, VPNs, VPLS, current trends and future developments. Fibernet; 2005: pp.1-16.

24. Madhusanka Liyanage, Mika Ylianttila. A novel distributed spanning tree protocol for provider provisioned VPLS networks. Next Generation Networking Symposium; 2014: pp.2982-2988.

25. Ethernet VPN and provider backbone bridging-EVPN: next generation solutions for MPLS-based Ethernet services [online]. Introduction and application note of Cisco ASR9000 Series Aggregation Services Routers; May 2014: pp.1-10.
URL: http://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/whitepaper_c11-731864.pdf.
Accessed 15 March 2015.

26. Ethernet VPN: Next Generation VPN [online]. Interoute Communications Limited website.
URL: http://www.interoute.com/product/ethernet-vpn-next-generation-vpn.
Accessed 18 March 2015.

27. BGP MPLS based Ethernet VPN [online]. Google Sites knowledge base.
URL: https://sites.google.com/site/amitsciscozone/home/important-tips/mpls-wiki/bgp-mpls-based-ethernet-vpn.
Accessed 20 February 2015.

28. Alastair Johnson. Ethernet VPN: next-generation VPN for Ethernet services [online]. Alcatel-Lucent Apricot; February 2014: pp.1-33.
URL: https://conference.apnic.net/data/37/2014-02-24-apricot-evpn-presentation_1393283550.pdf.
Accessed 20 March 2015.

29. Greg Hankins, Jorge Rabadan. Ethernet VPN for integrated layer 2-3 services [online]. Alcatel-Lucent website; 2 June 2014.
URL: http://www2.alcatel-lucent.com/techzine/ethernet-vpn-evpn-integrated-layer-2-3-services/.
Accessed 19 March 2015.

30. BGP MPLS based Ethernet VPN draft-ietf-l2vpn-evpn-11, work in progress [online]. 18 October 2014.
URL: https://tools.ietf.org/html/draft-ietf-l2vpn-evpn-11.
Accessed 15 March 2015.

31. BGP based multi-homing in VPLS draft-ietf-l2vpn-vpls-multihoming-07, work in progress [online]. 3 July 2014.
URL: https://tools.ietf.org/html/draft-ietf-l2vpn-vpls-multihoming-07.
Accessed 15 March 2015.

32. Introduction to carrier Ethernet VPNs: understanding the alternatives [online]. Juniper Networks white paper; May 2009.
URL: http://www.webtorials.com/main/resource/papers/juniper/paper1/carrier-ethernet-VPNs.pdf.
Accessed 10 March 2015.

33. Usage and applicability of BGP MPLS based Ethernet VPN draft-rp-l2vpn-evpn-usage-03, work in progress [online]. 14 October 2014.
URL: https://tools.ietf.org/html/draft-rp-l2vpn-evpn-usage-03.
Accessed 14 March 2015.

34. Requirements for Ethernet VPN [online]. IETF RFC 7209; May 2014.
URL: http://tools.ietf.org/html/rfc7209.
Accessed 14 March 2015.

35. BGP MPLS based Ethernet VPN [online]. IETF RFC 7432; February 2015.
URL: https://tools.ietf.org/html/rfc7432.
Accessed 14 March 2015.